Body Sensor Network Security

- Close coupling of BSNs and security
- why network security is important
- information is sensitive,
- what it takes to protect it,
- how its different from WSNs
- how encryption is executed on resource-constrained nodes

Applications: Home Monitoring

Source: http://www-03.ibm.com/technology/designconsulting/port_mhealth.html

- lots of deployed platforms, applications
- home monitoring
- BSN may interface to external network
- choice of interface decides security issues, convenience
- data coupling with originator
- wireless comm. ubiquitous in BSNs
- traditional wireless security issues persist

Why BSNs

- Required for long-term and continuous collection of data
- Optimize use of resources
- Enhances control, scheduling, and programming
- Adaptive to body condition and environment

- no longer just a matter of convenience
- emphasis on portable, wireless, non-intrusive
- data may not have to be analyzed before it comes off the BSN
- allows physicians, PCPs to monitor progress at home
- quantitative assessment

Why Secure

- Privacy
- Sensitive commands
- Delivery of service
- DoS attacks

- Security is a real concern
- Make choices about who sees the information
- Sensitive commands transferred in telemedicine,
- should verify the identity of the wearer before it delivers a service to him
- Five rights: PATIENT DRUG DOSE ROUTE TIME
- Do not send commands to a person nearby
- attacker could disrupt delivery of service
- Greatest concern is when WELL BEING is in the question
- Even in entertainment applications, interference is a concern
- Flood attack can deplete energy

Limitations

- WSN limitations are emphasized in BSNs
- Resource constraints
- Energy constraints

- Limitations emphasized in WSNs over BSNs
- Less resources available to implement security
- Energy harvesting possible but battery most likely used
- the working memory of a sensor node is not sufficient to even hold the variables for asymmetric cryptographic algorithms
- let alone perform operations with them.
- ENERGY -- how OFTEN do we have to authenticate?
- LOOK AHEAD

Competing Goals

Competing goals - should be portable, unobtrusive, non-disruptive to regular routine yet also secure

Secure Systems

- Random number generation
- Distribution channel

Why Not Wireless

- Bluetooth requires pre-shared secret as a basis for authentication
- UWB uses computationally expensive public-key mutual authentication
- ZigBee uses ACLs, high memory requirements

Why are existing wireless protocols unsuitable for BSNs?

WSNs vs. BSNs

- Authentication is intrinsic, essential to BSNs
- May be required by HIPAA
- Biological entropy lends itself to secure RNG
- Body-coupled communication inherently safer than wireless broadcast

Health Insurance Portability and Accountability Act -- Making use of biological entropy is context aware / physically aware computing

WSNs vs. BSNs (2)

- Pre-shared secret usually a “no-no”
- Implantable nodes difficult to “re-key”

IMPLANTABLE NODES
Pre-shared secrets are usually unacceptable because they can be snooped off the chip with an x-ray, but patients may be x-rayed, data can be stolen off chip

Existing Solutions: MobiHealth

- Inter-BAN communication
- Uses Bluetooth or ZigBee
- Could not address security

Other Existing Solutions

- COTS approach
- Computer-assisted physical rehabilitation
- Zigbee and sensors
- Security issues “remained a challenge”

Threat Sources

- Eavesdropping
- Injection
- Modification
- Interference

Overarching question [NEXT SLIDE]

How can nodes know that they belong to the same individual?

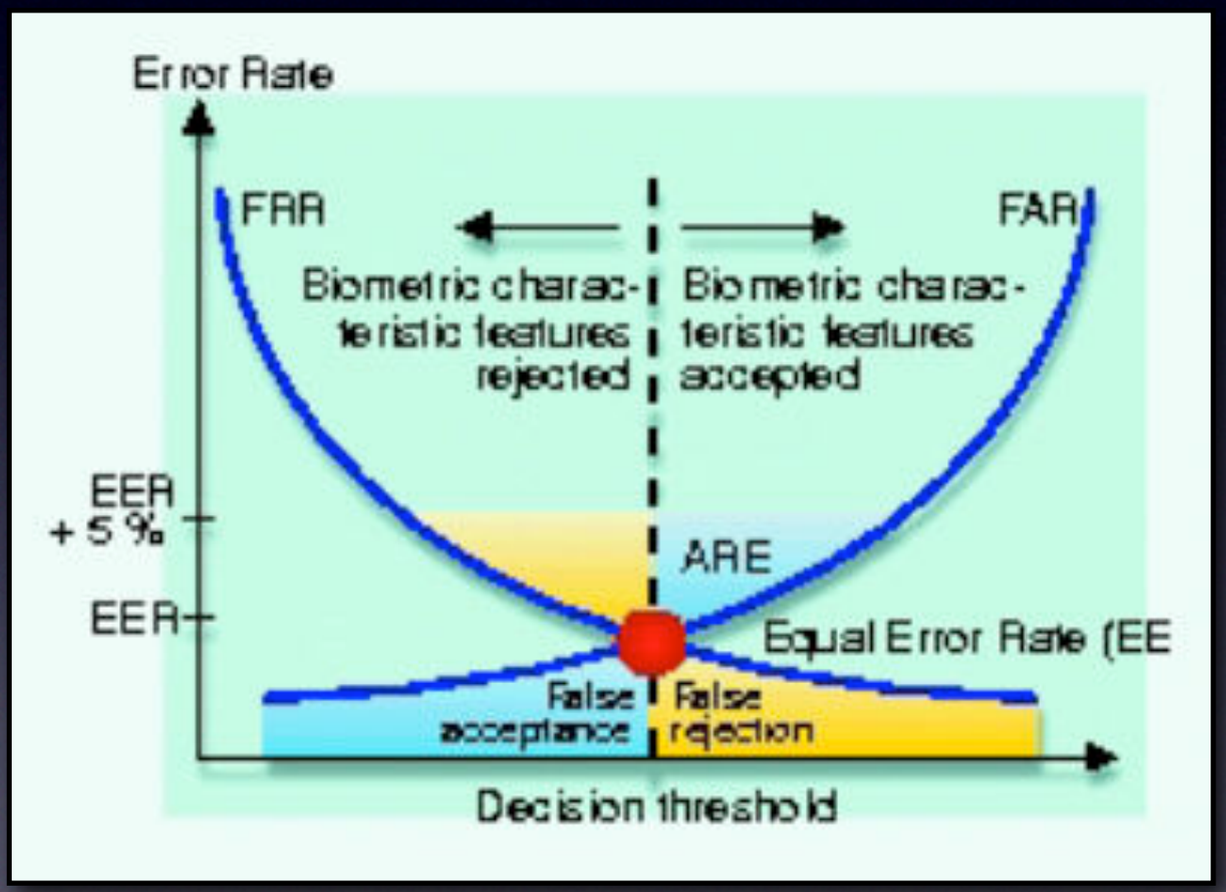
Biometrics to the rescue!!!11

Biometrics

- Identification by physiological trait
- Biometric measurement never perfect
- Hamming distance used for fuzzy commitment
- Performance characterized by FRR, FAR, EER

Biometric systems are characterized by False Rejection Rate, False Acceptance Rates, together described as the Equal Error Rate where FRR and FAR are the same

Performance Metrics



Biometric systems are characterized by False Rejection Rate, False Acceptance Rates, together described as the Equal Error Rate where FRR and FAR are the same

Performance Metrics

# of subjects	# of data segments	Sampling rate (Hz)	# of IPIs used/ binary sequence	Coding bits	Minimum HTER (%)	FRR (%)	FAR (%)
14	49	1000	67	128	0.01	0.00	0.03
85	789	1000	67	128	4.26	6.46	2.06
99	838	1000	67	128	2.58	3.99	1.18

Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
Face	n.a.	1 %	10 %	37437	Varied lighting, indoor/outdoor	FRVT (2002)[4]
Fingerprint	n.a.	1 %	0.1 %	25000	US Government operational data	FpVTE (2003)[5]
Fingerprint	2 %	2 %	2 %	100	Rotation and exaggerated skin distortion	FVC (2004)[6]
Hand geometry	1 %	2 %	0.1 %	129	With rings and improper placement	(2005)[7]
Iris	< 1 %	0.94 %	0.99 %	1224	Indoor environment	ITIRT (2005)[8]
Iris	0.01 %	0.0001 %	0.2 %	132	Best conditions	NIST (2005)[9]
Keystrokes	1.8 %	7 %	0.1 %	15	During 6 months period	(2005)[10]
Voice	6 %	2 %	10 %	310	Text independent, multilingual	NIST (2004)[11]

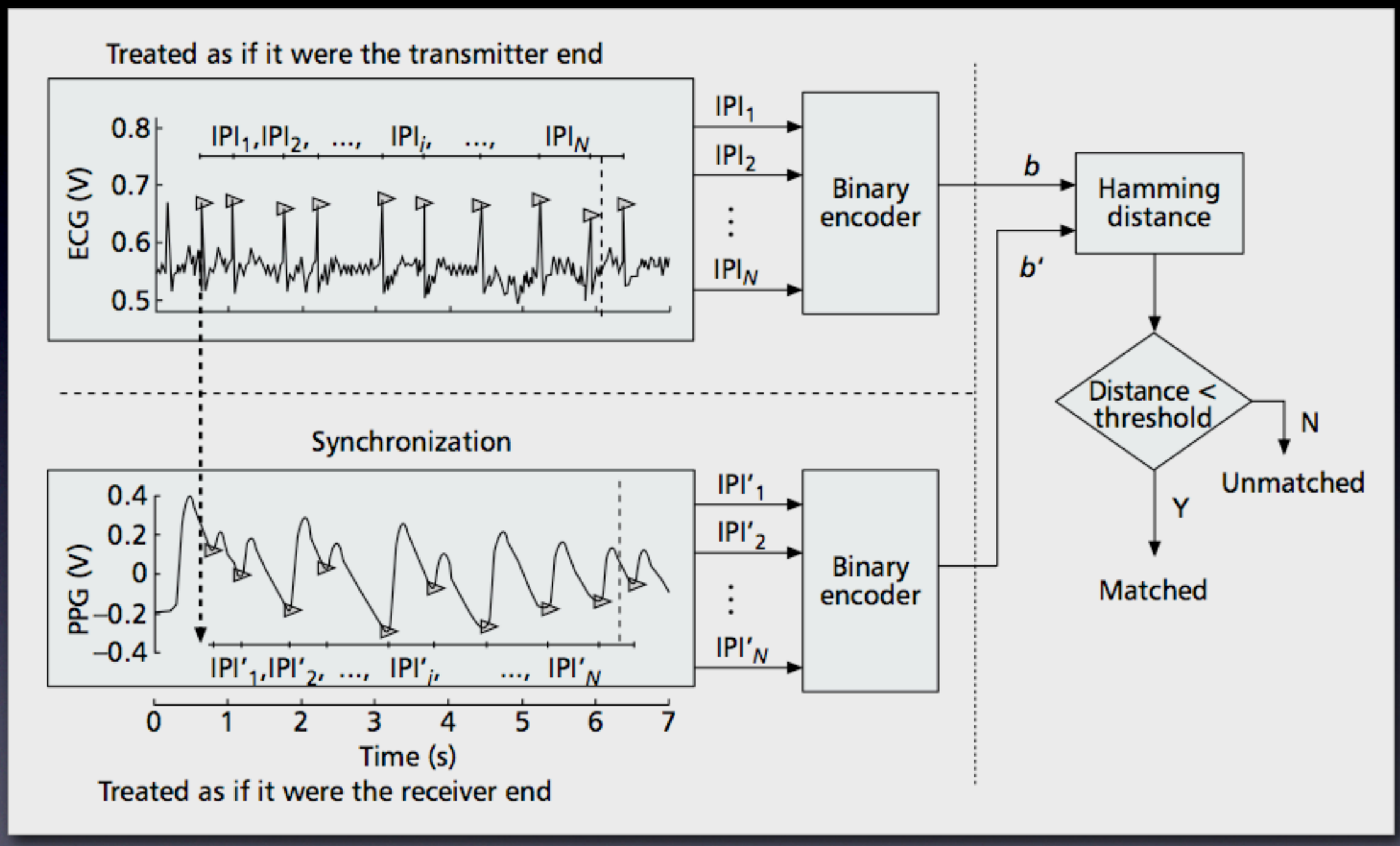
Compare performance numbers to existing biometric systems

Biometrics (2)

- Physiological characteristics identify the wearer
- Very difficult to forge
- Secured information pathways inside the body

Difficulty of forgery depends on trait chosen
Different from stored template,
-- continuously variable trait but
-- distinctive (different from person to person)
-- DIFFERENT FROM TYPICAL BIOMETRIC SYSTEMS

Synchronization of Biological Events



Experimenters prefer the use of interpulse interval due to high level of entropy, used Hamming distance to establish threshold of variance. Time synchronization signal may pose problem

Resource Constraints

- What about sensors that don't measure IPI?
- Is the increased complexity worth it?

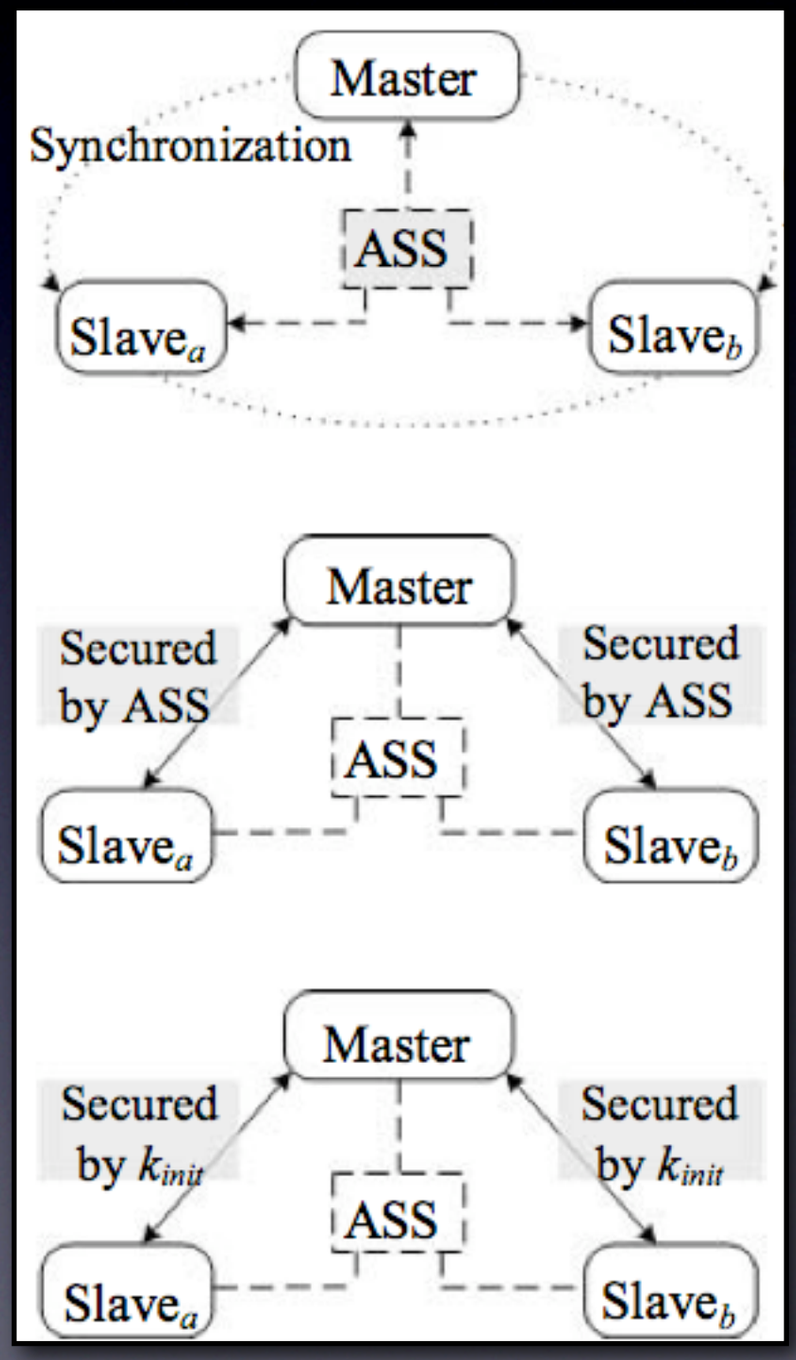
Experimenters suggest adding an extra sensor for authentication

The Other Paper

- RNG with thermal noise
- Auto-shared secret (unfortunate name) generated with IPI
- Bio-channel for auto shared secret distribution
- Nodes only need to encrypt data with secret

The Other Paper (2)

- Generation of network-wide ASS
- Initialization key distribution (under the protection of ASS)
- Session key distribution (under the protection of initialization key)



Dotted lines represent bio-channel

The Other Paper (3)

- Does bio-channel offer enough bandwidth?
- How does transmission power over bio-channel compare to wireless?
- What factors influence rate of authentication?
- What extra resources are needed for bio-channel communication?

Different key for each node = extra overhead

Conclusions

- Security and BSNs are closely coupled
- Traditional WSN technology not applicable in some cases
- Biometrics assure authenticity
- Bio-channel as transmission medium

BSNs inherently different from WSNs

Is the increased complexity worth it?
Discuss distribution of load in hardware / software
choosing a biometric trait